Department of Homeland Security Daily Open Source Infrastructure Report for 05 July 2006

Current Nationwide Threat Level is

ELEVATED
SIGNIFICANT RISK OF TERRORIST ATTACKS

For info click here
http://www.dhs.gov/

Daily Highlights

- The Associated Press reports that as the first workweek under a New Jersey state government shutdown began, more than half the state work force was off the job and those who were working might not get paid. (See item 25)

- KAIT reports Arkansas is one of four states in the nation that is developing a communication system going from analog to the new improved digital with the Arkansas Wireless Information Network, through an initiative by the Department of Homeland Security. (See item 29)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: ELEVATED, Cyber: ELEVATED

Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://www.esisac.com]

1. *July 03, Washington Post* — **Thousands without power Monday after fierce electrical storms.** More than 40,000 homes in the Washington area remained without power early Monday morning, July 3, after fierce electrical storms and torrents of rain tore down trees and branches throughout the waterlogged, storm−weary region Sunday night. Much of the damage was inflicted on the area's electrical grid. At one point after 10 p.m. EDT, Dominion Virginia Power reported 66,000 blacked−out homes; for Maryland's Pepco, the figure was 30,000. Baltimore Gas & Electric also reported thousands of outages. By 5 a.m. Monday, Dominion

Virginia Power was reporting 30,264 homes without power in Northern Virginia; Pepco reported 5,290 homes without power in Montgomery County, 2,544 homes without power in the District, and 1,320 homes without power in Prince George's County; and Baltimore Gas and Electric reported 1,161 homes without power in Anne Arundel County. James McIntyre, a spokesperson for the Federal Emergency Management Agency, said last night that there is no cap on the Federal reimbursement available to Maryland and that officials will consider other disaster designations −− including for individual assistance −− as they further assess the damage from storms that started two weekends ago.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07/03/AR2006070300187.html

2. *July 02, Boston Globe* — **Gaza breaking down without power plant.** When Israeli jets fired missiles at Gaza's only power plant last Wednesday morning, June 28, the airstrikes did not just knock out nearly half the electricity supply for 1.3 million Palestinians. They also triggered a domino effect that will lead to water shortages and sewage flooding within days, if Israelis do not allow in more fuel to power emergency generators, UN and Palestinian officials said. Engineers at the power plant said that the facility would take at least five months to repair, if not more. In Gaza, 70 percent of water pumps are now working on generator power, said Majed Abu Ramadan, the mayor. The strike initially knocked out power to 700,000 Gazans. The plant provided 90 megawatts of electricity, 43 percent of Gaza's power; the rest is delivered from Israel. Officials at Israeli and Palestinian electric utilities said that Israel could not cover the shortfall because electric lines connecting Gaza to Israeli power sources do not have the capacity. The transformers are not available off the shelf and will take months to produce.
Source: http://www.iht.com/articles/2006/07/02/news/power.php

3. *July 02, Calgary Herald* — **Great Plains producers feel the pain.** Some U.S. wells have been shut down and others are in danger of closing. The culprit is a flood of cheaper Canadian crude which, instead of replacing supply from members of the Organization of the Petroleum Exporting Countries (OPEC), is replacing oil production in states close proximity to Canada. Producers in several Great Plains states say refinery customers are replacing their product with Canadian crude. They say it's becoming more difficult to ship their oil to other markets because the cheaper Canadian product is crowding them out of pipelines. Domestic oil is being discounted as much as 40 percent in such states as Montana, Wyoming, and North Dakota −− giving small producers there less than what Big Oil companies and OPEC members are getting. Therefore, some projects to drill new wells are being postponed or reconsidered, and wells are being closed. Some owners of oil wells, who have farmed out the production to the oil companies, have received letters saying their wells may have to be shut down. The states thought to be most affected are Colorado, Montana, North Dakota, South Dakota, Utah, and Wyoming, which are served by pipelines from Canada.
Source: http://www.canada.com/calgaryherald/news/calgarybusiness/story.html?id=aa85a147−2871−4173−a391−0e66f535d9e2

4. *July 02, Boston Globe* — **Radioactive parts are no longer missing.** The radioactive parts reported missing at Pilgrim Nuclear Power Station in May have been found. The nine pen−sized radioactive neutron detectors that could not be located during a routine cleanup of the plant's spent fuel pool were, in fact, sent to a low−level radioactive waste facility years ago, the plant reported to the Nuclear Regulatory Commission (NRC) late last month. The inventory

list was never updated to reflect that the detectors were removed from the reactor. NRC spokesperson Neil Sheehan said the commission was reviewing how the “record−keeping breakdown” occurred, and would later decide whether to take enforcement action or administer penalties.
Source: http://www.boston.com/news/local/articles/2006/07/02/radioactive_parts_are_no_longer_missing/

5. *July 02, Miami Herald* — **Energy sector reviews lessons from storms.** With weather forecasters expecting an "above average" hurricane season, government regulators and major players in the energy sector hope errors made last year during Hurricanes Katrina and Rita won't be repeated. Energy companies have spent months honing their response plans to include the hard lessons learned from Katrina and Rita. The inability to communicate with key personnel and the authorities was a principal problem last year. Now, at Shell's Texas and Louisiana onshore operations, key personnel are armed with satellite phones and Black Berrys, which allow text messaging even when cell towers have been destroyed. "The biggest lesson we learned is we need to start earlier," said Colleen Hutchings, the health and safety director at Deer Park. Critical employees now will be sent home five days before a storm's potential landfall to prepare their homes and move their families so that they can return to work and focus on storm plans that could affect national fuel supplies. This year, critical energy employees in the Houston area have been given special ID badges. Law enforcement agencies have been instructed to recognize these badges and allow their holders back in.
Source: http://www.miami.com/mld/miamiherald/business/14948030.htm

6. *July 01, Japan Times* — **Halted reactor in Shizuoka yields broken turbine blades.** Fifty turbine blades have been found cracked or broken in a Chubu Electric Power Co. nuclear reactor in Shizuoka Prefecture, the company said Friday, June 30. The damaged blades were found in two of three low−pressure turbines of the No. 5 reactor at the Hamaoka nuclear plant in Omaezaki after an automatic shutdown of the 1,380−megawatt boiling water reactor on June 15 following excessive vibration in the turbines. Of 139 blades in the first turbine, excluding those that came off, 28 were partially broken and 18 were cracked, the utility said. Four blades installed in the second turbine were also found damaged. Company officials investigating the shutdown said the number of blades that have broken or cracked is expected to increase as the probe is continuing. Hitachi Ltd., which manufactured the turbines, said it believes the cracks resulted from a design problem.
Source: http://search.japantimes.co.jp/cgi−bin/nn20060701a7.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

7. *July 03, Associated Press* — **Thieves release toxic cloud.** Two thieves released a toxic cloud of anhydrous ammonia early Monday, July 3, after they tried to steal the chemical used in fertilizer and to make methamphetamine. The cloud forced residents in rural Bartholomew County, IN, to stay inside their homes for at least two hours while rescue workers tried to close a leaking seal on one of two seven−gallon tanks that were used to siphon the chemical. Sheriff’s deputies shot the tanks after they could not close the leaking valve.
Source: http://www.indystar.com/apps/pbcs.dll/article?AID=/20060703/ NEWS01/60703032

8. *July 02, KTRK TV (TX)* — **Explosion and fire at chemical plant prompts shelter−in−place warning.** ExxonMobil says no dangerous chemicals were released into the air after an explosion Sunday, July 2, at a Baytown, TX, plant. Officials report there was an explosion in the plant's rubber processing unit followed by a fire. A shelter−in−place order was issued to those in the vicinity while crews put out the blaze. Near−by residents say they could feel the blast that knocked out their power for a while.
Source: http://abclocal.go.com/ktrk/story?section=local&id=4327618

[Return to top]

Defense Industrial Base Sector

9. *July 05, European Defense Agency* — **Birth of European Defense Equipment Market with launch of Code of Conduct.** A new era for defense procurement in the European Union (EU) began on Saturday, July 1, with the introduction of a regime designed to increase transparency and competition in the European Defense Equipment Market, offer armed forces and taxpayers better value for money, broaden business opportunities for defense companies and strengthen the global competitiveness of the European industry. "For the first time ever, European countries have committed to procure defense equipment from each other if the offer is the best available, instead of automatically contracting with a national supplier," said Javier Solana, EU High Representative for the Common Foreign and Security Policy and Head of the European Defense Agency.
Procurement opportunities will be publicized through a new Electronic Bulletin Board: http://www.eda.europa.eu/ebbweb/
Source: http://www.eda.europa.eu/news/2006−06−30−0.htm

10. *June 30, GovExec* — **Defense IG to release reports on interagency contracting problems.** Faulty contracting practices and violations of a law on federal spending will be the subject of five reports to be released in August by the Department of Defense (DoD) inspector general's (IG) office, a Defense official told an acquisition advisory group Thursday, June 29. Terry McKinney, program director for the contract management directorate at DoD's IG office, said the office is completing work on four separate reports on Defense contracts placed through the General Services Administration, procurement centers at the Interior and Treasury departments, and NASA. A fifth report will focus on about 70 violations of the Anti−Deficiency Act uncovered in fiscal 2005 and also will address about 38 violations from fiscal 2004 that were previously disclosed, he said. The Anti−Deficiency Act prevents agencies from spending funds in excess of a given appropriation.
Source: http://www.govexec.com/story_page.cfm?articleid=34464&dcn=to daysnews

[Return to top]

Banking and Finance Sector

11. *July 02, Associated Press* — **Students at Missouri Southern alerted to 'exposure' of personal data.** Social Security numbers and other personal information of some students at

Missouri Southern State University have been exposed, university officials said. Information included Social Security number, phone number, grade−point average, and user identification number. Richard McCallum, vice president of academic affairs, said no evidence any of the information had been used to the potential harm of students. McCallum said he did not know the date of the exposure or when the university discovered the problem, but he said officials took immediate action after learning about it from a student.
Source: http://www.newstribune.com/articles/2006/07/03/news_state/18 2state12data.txt

12. *July 01, Washington Post* — **Five arrested in theft of LexisNexis data.** Federal authorities last week arrested five men in connection with a 2005 network breach at LexisNexis Group that the database giant said led to the theft of personal records on more than 310,000 individuals. The government charges that the men also used stolen or illegally created accounts at LexisNexis subsidiaries to look up Social Security numbers and other personal information on dozens of celebrities. The government alleges that on two dates in January and March 2005, one of the men compromised a computer belonging to an officer in the Port Orange, FL, Police Department. He then allegedly used the department's credentials to access records at Accurint, a database service for law enforcement and legal professionals offered by Seisint, a Florida−based subsidiary of LexisNexis. The indictment charges that he used that access to create even more user accounts, which he then allegedly shared with the other co−defendants. The indictment also alleges that at the same time, another defendant gained access to an Accurint account belonging to a police department in Denton County, TX, by impersonating a LexisNexis employee. The group allegedly accessed information on Hilton, California Governor Arnold Schwarzenegger (R), and actors Laurence Fishburne and Demi Moore.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/06/30/AR2006063001784.html

13. *June 29, Lincoln Journal Star* — **Hacker breaks into Nebraska Treasurer's Office.** Personal and financial information of more than 300,000 people and 9,000 employers may be in the hands of a hacker following a Wednesday, June 28, break−in of the state computer system that processes child−support payments. A preliminary investigation of the incident suggests that the hacker did not download the information, said State Treasurer Ron Ross. But the possibility does exist. "Based upon the method of attack, it is more likely the hacker's intent was not to steal information, but rather to do something malicious since the hacker inserted a virus onto the server, which we immediately removed," Ross said. KidCare, the child−support payment system, processes $1 million in transactions daily. Identity information potentially stolen by the hacker, which investigators believe may be based outside the U.S. and possibly in Asia, includes: names, addresses, bank account numbers, social security numbers, and tax identification numbers. The State Patrol has initiated a full investigation that could include help from the FBI and other agencies.
Source: http://www.journalstar.com/articles/2006/06/29/local/doc44a3fa6c4f795799631319.txtj

[Return to top]

Transportation and Border Security Sector

14.

July 04, Associated Press — **Spain mourns 41 train crash victims.** Spain was in mourning Tuesday, July 4, after a subway train accelerated, shuddered, and flipped off the tracks in the Mediterranean port of Valencia −− a city of 800,000 people about 220 miles southeast of Madrid −− on Monday, July 3, killing at least 41 and injuring 47 others. Regional authorities and a witness said the train was going too fast and one of its wheels broke into pieces, derailing the first car, which overturned. The accident brought back memories of the 2004 terrorist attack on Madrid commuter trains that killed 191 people. It was the second accident on Valencia's No. 1 line in less than a year. A September collision involving three trains injured at least 30 people, four of them seriously. Jorge Alvarez, secretary−general of the Independent Railway Union, said it was too early to blame human error for Monday's tragedy. He said his union repeatedly warned of safety problems on Valencia's 18−year−old subway system, particularly the No. 1 line. More than 60 million people used Valencia's subway system in 2005, some 165,000 people a day, according to its Website. The subway has four lines and 116 stations.
Source: http://www.cnn.com/2006/WORLD/europe/07/04/spain.crash.ap/in dex.html

15. *July 03, USA TODAY* — **Struggling Delta, Northwest dump flights.** Delta and Northwest airlines have shed more flights in the last 12 months than any other U.S. carriers as the two troubled companies scramble to cut costs and match offerings with traveler demand. This month, Delta is offering 14 percent fewer flights than in July 2005 and Northwest is offering 15 percent fewer, according to a USA TODAY analysis of schedule data from Back Aviation Solutions. Combined, the airlines and their affiliated carriers have cut more than 1,000 flights a day from July 2005. Those reductions −− and cutbacks by other big airlines −− are contributing to this summer's crowded air travel experience for U.S. travelers, with well over 80 percent of the average flight's seats occupied. Northwest and Delta filed for bankruptcy protection on the same day last September. Neither expects to exit until next year. The analysis shows that the airlines' managements have made some similar judgments in deciding how to pare back. To a large extent, Delta and Northwest are late paring back. Most competitors made their move after the collapse of travel following the September 11 terrorism.
Source: http://www.usatoday.com/travel/flights/2006−07−02−air−cuts−u sat_x.htm

16. *July 03, North Jersey Media Group* — **Amtrak's power crunch.** Increasingly, power problems are affecting train service in New Jersey, where the busiest track is owned by Amtrak but heavily used by NJ Transit. The number of power−related train delays on Amtrak−owned tracks in New Jersey has increased 64 percent between 2000 and 2006, according to NJ Transit. The total bill to upgrade the electric system is $370 million, according to a five−year plan Amtrak published last year. Some of the most common delays are caused by old catenary wire, which sags when the weather turns hot. Trains must slow down or the train's pantograph, a Z−shaped arm that collects electricity from the wire, could pull down the catenary. Stephen Nagy, a retired conductor who left NJ Transit in 2003, said catenary problems in the summer are frequent and disruptive. He said trains between Trenton and New York are often ordered to reduce their speed from 135 to 80 mph. This year, for the first time, Congress directed all commuter railroads to pay a fee to Amtrak for their use of the Northeast Corridor. NJ Transit has invested $300 million on corridor improvements since 1996. Amtrak has spent about $400 million a year on capital improvements, said Cliff Black, an Amtrak spokesperson.
Source: http://www.northjersey.com/page.php?qstr=eXJpcnk3ZjczN2Y3dnF
lZUVFeXkzJmZnYmVsN2Y3dnFlZUVFeXk2OTU2NzYyJnlyaXJ5N2Y3MTdmN3Z
xZWVFRXl5Mg==

17. *July 03, Associated Press* — **Cost of new baggage−screening system causing conflict in Phoenix.** Phoenix officials and the federal government are at odds over who should foot the bill for extra costs of what was supposed to be a $122 million baggage−screening system at Phoenix Sky Harbor International Airport. The system is now projected to cost $143 million and is considered crucial to the airport's operations because it will allow security screeners to scan checked baggage for explosives and other prohibited items more quickly and out of sight of the congested passenger terminals. The airport screens 40,000 or more bags a day. Under a 2004 agreement, Sky Harbor officials had pledged to front the money for the system with the understanding that the federal government would reimburse them $91.5 million, or 75 percent. At least a dozen more airports have approved plans for the technology and are waiting for funding. The Transportation Security Administration, however, has not signed any more agreements because there isn't enough money to go around. The machines, which can cost up to $1 million each, have also caused operational problems for Sky Harbor and other busy airports. Some are as large as minivans and take up huge amounts of space in congested check−in areas.
Source: http://www.usatoday.com/travel/flights/2006−07−03−phoenix−ai rport−security_x.htm

18. *June 28, Minneapolis/St Paul Business Journal* — **Northwest Airlines to speed retirement of DC−10 planes.** Northwest Airlines Corp. said Wednesday, June 28, that it will speed up the retirement of its DC−10 aircraft to save fuel and lower maintenance costs as it attempts to emerge from Chapter 11 bankruptcy protection. Eagan, MN−based Northwest is phasing out its remaining 12 DC−10 planes throughout the next seven months and replacing them with new Airbus A330s and Boeing 747−400 planes. The Airbus jets will provide up to 30 percent fuel savings, fit in more passengers, and run more quietly than the DC−10s.
Source: http://biz.yahoo.com/bizj/060629/1308212.html?.v=3

[Return to top]

Postal and Shipping Sector

Nothing to report.

[Return to top]

Agriculture Sector

19. *July 03, Baraboo News Republic (WI)* — **Devil's Lake deer had chronic wasting disease.** The Wisconsin Department of Natural Resources announced Friday, June 30, that officials killed a deer testing positive for chronic wasting disease (CWD) at Devil's Lake State Park in April. Park staff shot the deer because of its emaciated appearance, which is an indicator of CWD in the late stages. Since 2002, 651 wild white−tailed deer have tested positive for CWD in Wisconsin. This is the seventh afflicted deer found in Sauk County.
CWD information: http://www.cwd−info.org/
Source: http://www.wiscnews.com/bnr/news/index.php?ntid=89665&ntpid= 0

20. *July 03, United Nations News Service* — **Developing countries need help in preserving vital agricultural biodiversity.** With crucial agricultural genetic resources at risk, developing

countries should be enabled to fully exploit biotechnology tools to stop the decline of biodiversity and use their wealth of such resources as an insurance against climatic and other changes, according to a new United Nations study. Crop, forest, animal and fish genetic resources represent an insurance against future changes in production and climatic conditions or in market needs, but they are endangered by such factors as overexploitation, replacement of local crops and livestock with foreign species or breeds and habitat change and destruction, the Food and Agriculture Organization noted. The study seeks to shed light on the potential role and importance that biotechnology tools, in particular the use of molecular markers, may have for agricultural genetic resources in developing countries. New and old biotechnologies provide a broad collection of tools that can be applied for a range of different purposes such as genetic improvement, disease diagnosis, and vaccine development.
The Role of Biotechnology in Exploring and Protecting Agricultural Genetic Resources: ftp://ftp.fao.org/docrep/fao/009/a0399e/a0399e00.pdf
Source: http://www.un.org/apps/news/story.asp?NewsID=19076&Cr=&Cr1=

21. *July 03, Animal and Plant Health Inspection Service* — **Web−based permit system expanded.** The U.S. Department of Agriculture’s Animal and Plant Health Inspection Service (APHIS) Monday, July 3, expanded its new electronic permitting system to include online applications for permits issued by Veterinary Services’ National Center for Import and Export. APHIS ePermits is a Web−based system designed to improve and expedite the permitting process. Under ePermits, applicants can apply for permits, track applications and receive notifications, as well as copies of their permits −− all through the Internet. APHIS first launched ePermits on April 3. At that time, certain permits applications from APHIS’ plant protection and quarantine and biotechnology regulatory services programs were made available online. This latest expansion of ePermits will allow customers to apply for several frequently requested Veterinary Services' permits online.
ePermits information: http://www.aphis.usda.gov/permits/learn_epermits.shtml
Source: http://www.aphis.usda.gov/newsroom/content/2006/07/web−based _permits.shtml

[Return to top]

Food Sector

22. *July 02, Independent (United Kingdom)* — **Salmonella bug may have affected up to thirty brands.** The salmonella food poisoning bug found in Cadbury chocolate, in England, may have contaminated up to 30 different brands, food safety officials have warned. Safety tests are now being carried out on a wide range of bars after it emerged that the contamination, which was caused by a leaking pipe discovered earlier this year at a Cadbury plant, may have been far greater than first realized. More than one million Cadbury chocolate bars were withdrawn from sale 10 days ago after the firm admitted that chocolate "crumb" was contaminated with traces of salmonella montevideo, a rare strain of the bug, six months ago. Health officials in Birmingham are now testing another 30 brands and the Food Standards Agency has warned that other types of Cadbury chocolate could be withdrawn.
Source: http://news.independent.co.uk/uk/health_medical/article11536 40.ece

[Return to top]

Water Sector

Nothing to report.
[Return to top]

Public Health Sector

23. *July 03, Reuters* — **Bird flu kills fortieth human in Indonesia.** A World Health Organization (WHO) laboratory test has confirmed a five−year−old Indonesian boy who died last month was infected with bird flu, a Health Ministry official says. His death takes the total number of confirmed bird flu fatalities in the country to 40. I Nyoman Kandun, director general for communicable disease control at the Health Ministry, told Reuters the victim died on June 16 in Tulungagung in East Java province after being admitted to hospital on June 8.
Source: http://www.abc.net.au/news/newsitems/200607/s1677832.htm

24. *July 03, Reuters* — **Manufacturer warned over flu shot plant problems.** The U.S. Food and Drug Administration (FDA) sent a warning letter to a Sanofi−Aventis unit over manufacturing problems related to its FluZone flu vaccine, agency officials said on Monday, July 3. Some batches of vaccine ingredients made at a Pennsylvania plant failed sterility tests, the FDA said. None of those batches were used to make final vaccine products, the FDA said.
FDA letter: http://www.fda.gov/foi/warning_letters/g5899d.pdf
Source: http://today.reuters.co.uk/news/newsArticle.aspx?type=healthNews&storyID=2006−07−03T161207Z_01_WAT005978_RTRIDST_0_HEALTH−SANOFI−VACCINE−DC.XML

[Return to top]

Government Sector

25. *July 03, Associated Press* — **New Jersey government shutdown.** As the first workweek under a state government shutdown began, more than half the state work force was off the job and those who were working might not get paid. Governor Jon S. Corzine imposed the shutdown after lawmakers missed a July 1 deadline to adopt a new state budget. The impasse among Democrats over a sales tax increase left New Jersey with no means to spend money. No budget bills had moved through legislative committees yet, and any legislation those panels approve must wait a full calendar day before receiving final votes in the Assembly and Senate. If no bills move forward Monday, the Legislature couldn't adopt a budget before Wednesday morning. New Jersey's courts didn't open Monday, July 3, lottery ticket sales were shut down, and the same could happen to betting at racetracks and the Atlantic City casinos. By Wednesday, state parks and beaches could also be closed. Racetracks and casinos, which require state monitoring, will be closed Wednesday if no budget is enacted by then. If the shutdown drags on, Corzine said, services funded with state aid, such as prescription drug assistance and hospitals, will also be hit.
Source: http://www.washingtonpost.com/wp−dyn/content/article/2006/07/03/AR2006070300169.html

[Return to top]

Emergency Services Sector

26. *July 03, U.S. Department of Defense* — **NORTHCOM, Canada Command cooperate to respond to disasters in North America.** U.S. Northern Command (NORTHCOM) has a new partner in defending North America from future terrorist and natural disasters. During his first official visit to NORTHCOM headquarters as the commander of Canada Command, Canadian Forces Lt. Gen. Marc Dumais promised the two nations would take their already strong military cooperation to new heights. Canada Command is the Canadian Forces formation responsible for all of Canada's routine and contingency domestic operations. The creation of Canada Command was based on the new international security environment and a commitment to place greater emphasis on the defense of Canada and North America. Dumais stressed the importance of being prepared to deal with an "event of magnitude" that crosses the U.S.−Canada border in an effective binational and bilateral way. The relationship between the two commands will enhance support between the nations during events like Hurricane Katrina last year in the United States and the 1998 Canadian ice storm, he added.
Source: http://www.defenselink.mil/news/Jul2006/20060703_5565.html

27. *July 02, Federal Emergency Management Agency* — **President declares major disaster for Pennsylvania, New York, Ohio, Maryland.** The head of the U.S. Department of Homeland Security's Federal Emergency Management Agency has announced that federal disaster aid has been made available for Pennsylvania, New York, Ohio, and Maryland due to recent storms and flooding. For more information:
Pennsylvania Severe Storms, Flooding, and Mudslides:
http://www.fema.gov/news/event.fema?id=6465
New York Severe Storms and Flooding: http://www.fema.gov/news/event.fema?id=6485
Ohio Severe Storms, Tornadoes, Straight Line Winds, and Flooding:
http://www.fema.gov/news/event.fema?id=6505
Maryland Severe Storms, Flooding, and Tornadoes:
http://www.fema.gov/news/event.fema?id=6506
Source: http://www.fema.gov/news/disasters.fema#diz

28. *July 02, Virginian−Pilot* — **Equipment shortages are strain on the Guard, Virginia officials say.** As Virginians brace for another hurricane season, there's concern that Army National Guard troops lack some key equipment needed for emergency operations. Both state and federal officials acknowledge widespread shortages of materiel after four years of steady overseas deployments by the country's Reserve soldiers and airmen. Virginia Army National Guard officials say the state needs more trucks, helicopters and radios. Unit commanders say the deficiencies have forced changes to training schedules and prompted searches for more equipment. Despite this, state officials say the Guard can respond effectively to a natural disaster or potential terrorist attack.
Source: http://home.hamptonroads.com/stories/story.cfm?story=106981& ran=117534

29. *June 26, KAIT 8 (AR)* — **Arkansas developing digital communication system.** Arkansas is one of four states in the nation that is developing a digital communication system through an

initiative by the Department of Homeland Security. The state of Arkansas is taking communication from old analog to the new improved digital with the Arkansas Wireless Information Network (AWIN). The first phase of the project was upgrading the existing Arkansas State Police network to use as a backbone for AWIN. The second phase of the project was putting up new towers around the state to better enhance coverage. Currently, only the Arkansas State Police are using the system, however the state is expecting other emergency personnel to begin integrating this technology when it is turned on sometime in the fall.
Source: http://www.kait8.com/Global/story.asp?S=5081372&nav=0jsh

[Return to top]

Information Technology and Telecommunications Sector

30. *July 03, VNUNet* — **Volume of e−mail viruses falls in June.** The percentage of e−mails containing viruses remained at just 0.36 percent during June, despite an attack launched by the Bagle virus. The percentage of spam, however, was marginally higher month on month at 85.11 percent, according to figures from anti−spam and antivirus firm SoftScan. SoftScan considers this change to be the result of less business related e−mail as the holiday season begins, rather than an overall increase in spam.
Source: http://www.vnunet.com/vnunet/news/2159571/volume−email−virus es−falls−june

31. *July 03, VNUNet* — **OpenOffice patches three security holes.** OpenOffice.org has released an update for its open source productivity suite that plugs three security vulnerabilities. Security Website Secunia rated the vulnerabilities as "moderately critical," its third most severe designation on a five−step scale. The vulnerabilities affect OpenOffice versions 2 and 1.1.5. An update for version 2 is available for download now. A patch for the previous version will be released shortly.
Secunia advisory: http://secunia.com/advisories/20867/
Source: http://www.vnunet.com/vnunet/news/2159541/openoffice−patches −three

32. *July 03, VNUNet* — **Netsky blown away in June virus charts.** Netsky.q has been pushed off the top of the virus charts for the first time since 2004, according to monthly statistics released by Kaspersky Lab. Netsky.q has been the most widespread e−mail worm since 2004 and its variant Netsky.t has risen rapidly since the beginning of 2006. However, both worms fell away sharply in June, with Netsky.q falling to 15th place and Netsky.t to 20th. Kaspersky Lab said that it was possible that both worms will disappear entirely from the company's next top 20 list in July. The other surprise in June was that Nyxem.e returned to the charts, becoming the second most encountered virus.
Kaspersky Lab's Virus Top Twenty for June 2006:
http://www.kaspersky.com/news?id=189806199
Source: http://www.vnunet.com/vnunet/news/2159533/netsky−virus−blown −away−virus

33. *June 30, Secunia* — **Cisco Wireless Control System multiple vulnerabilities.** Some vulnerabilities and a security issue have been reported in Cisco Wireless Control System (WCS), which can be exploited by local users to gain knowledge of sensitive information, and to gain knowledge of sensitive information, conduct cross−site scripting attacks, bypass certain

security restrictions and potentially compromise a vulnerable system.
Affected software: Cisco WCS 1.x.
Solution: Update to WCS for Linux and Windows 3.2(63) or later:
http://www.cisco.com/public/sw−center/sw−usingswc.shtml
Default administrator passwords should be changed after installation.
Source: http://secunia.com/advisories/20870/

34. *June 30, IDG News Service* — **Worm appears as Microsoft antipiracy program.** Security analysts have detected a new piece of malware that appears to run as a Microsoft program used to detect unlicensed versions of its operating system. The malware has been classified as a worm and spreads through AOL's Instant Messenger program, said Graham Cluley, senior technology consultant for Sophos. Sophos is calling it W32.Cuebot−K, a new variation in the Cuebot family of malware. After it's installed, the worm immediately tries to connect to two Websites, a sign it may try to download other bad programs on the machine.
Source: http://www.infoworld.com/article/06/06/30/HNwormmsantipiracy_1.html

35. *June 29, InfoWorld* — **EMC to buy RSA Security for $2.1 billion.** EMC, in a bold move to buttress its information management technologies with world−class data protection and access management, has agreed to buy RSA Security for about $2.1 billion in an all−cash transaction, the companies announced on Thursday, June 29. Through the acquisition, EMC adds identity and access management, encryption, and key management software to its security portfolio.
Source: http://www.infoworld.com/article/06/06/29/27NNrsa_1.html

36. *June 21, U.S. Computer Emergency Readiness Team* — **US−CERT Vulnerability Note VU#394444: Microsoft Hyperlink Object Library stack buffer overflow.** There is a stack−based buffer overflow in the Microsoft Hyperlink Object Library (HLINK.DLL). The overflow may be triggered by clicking a specially crafted hyperlink. Note that any program that links to the HLINK.DLL library may be vulnerable, including Microsoft Office applications. Exploit code for this vulnerability is publicly available. By convincing a user to access a specially crafted hyperlink, an attacker could execute arbitrary code with the privileges of the attacked user. If the user is logged in with administrative privileges, the attacker could take complete control of a vulnerable system.
Solution: Do not click on unsolicited links received in e−mail or embedded in Office documents. Exploitation of this vulnerability requires a user to click a specially crafted link. By only accessing hyperlinks from known and trusted sources, the chances of exploitation are reduced. There is currently no patch or update to correct this problem.
Source: http://www.kb.cert.org/vuls/id/394444

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

US−CERT Operations Center Synopsis: US−CERT is aware of publicly available exploit code for two unpatched vulnerabilities in Microsoft Internet Explorer. By persuading a user to double click a file accessible through WebDAV or SMB, a remote attacker may be able to execute arbitrary code with the privileges of the user. US−CERT is tracking the first vulnerability as VU#655100:
http://www.kb.cert.org/vuls/id/655100

The second issue is a cross domain violation vulnerability that is being tracked as VU#883108: http://www.kb.cert.org/vuls/id/883108

Successful exploitation could allow a remote attacker to access the contents of a web page in another domain. This exploitation could lead to information disclosure, which may include harvesting user credentials. Until an update, patch, or more information becomes available, US−CERT recommends the following:

Do not follow unsolicited links.

To address the cross domain violation vulnerability (VU#883108):
http://www.kb.cert.org/vuls/id/883108

Disable ActiveX as specified in the Securing Your Web Browser:
http://www.us−cert.gov/reading_room/securing_browser/#Intern et_Explorer

Review Malicious Web Scripts FAQ:
http://www.cert.org/tech_tips/malicious_code_FAQ.html#steps

US−CERT will continue to update current activity as more information becomes available

Public Exploit Code for Unpatched Vulnerability in MS Office Hyperlink Object Library

US−CERT is aware of publicly available exploit code for an unpatched buffer overflow vulnerability in Microsoft Hyperlink Object Library (HLINK.DLL). By persuading a user to access a specially crafted hyperlink in an email message or MS Office document, a remote attacker may be able to execute arbitrary code with the privileges of the user.More information about this vulnerability can be found in the following:

VU#394444 − Microsoft Hyperlink Object Library stack buffer overflow:
http://www.kb.cert.org/vuls/id/394444

Until an update, patch, or more information becomes available, US−CERT recommends the following:

Do not follow unsolicited web links received in email messages or embedded in MS Office documents.

US−CERT will continue to update current activity as more information becomes available.

PHISHING SCAMS

US−CERT continues to receive reports of phishing scams that target online users and Federal government web sites. US−CERT encourages users to report phishing incidents based on the following guidelines:

Federal Agencies should report phishing incidents to US−CERT. http://www.us−cert.gov/nav/report_phishing.html

Non−federal agencies and other users should report phishing incidents to Federal Trade Commissions OnGuard Online. http://onguardonline.gov/phishing.html

Current Port Attacks

Top 10 Target Ports	1026 (win−rpc), 7674 (−−−), 445 (microsoft−ds), 38566 (−−−), 24232 (−−−), 4672 (eMule), 54856 (−−−), 25 (smtp), 19008 (−−−), 26777 (−−−) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

Commercial Facilities/Real Estate, Monument &Icons Sector

Nothing to report.

[Return to top]

General Sector

Nothing to report.

[Return to top]

DHS Daily Open Source Infrastructure Report Contact Information

DHS Daily Open Source Infrastructure Reports − The DHS Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary of open−source published information concerning significant critical infrastructure issues. The DHS Daily Open Source Infrastructure Report is archived for ten days on the Department of Homeland Security Website: http://www.dhs.gov/iaipdailyreport

DHS Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS Daily Report Team at (703) 983−3644 for more information.

Contact DHS

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

Department of Homeland Security Disclaimer

The DHS Daily Open Source Infrastructure Report is a non−commercial publication intended to educate and inform personnel engaged in infrastructure protection. Further reproduction or redistribution is subject to original copyright restrictions. DHS provides no warranty of ownership of the copyright, or accuracy with respect to the original source material.